



هویت و امنیت سایبری

ICS

Identity and Cyber Security

افزایش مهارت‌های عمومی کاربران فضای مجازی

مؤلف : غلامرضا نخعی نیازی

سرشناسه

نخعی، غلامرضا، ۱۳۵۱ -

عنوان و نام پدیدآور : هویت و امنیت سایبری: افزایش مهارت های عمومی کاربران فضای مجازی ICS: identity and

cybersecurity مؤلف غلامرضا نخعی نیازی

مشخصات نشر

تهران: فرهنگ روز، ۱۳۹۳.

مشخصات ظاهری

۲۷۲ ص: مصور، جدول، نمودار

شابک

978-600-6330-26-6

فهرست نویسی

فیبیا

موضوع

فضای مجازی - کامپیوترها - جرایم کامپیوتری - تدابیر اطلاعات - تدابیر ایمنی

رده بندی کنگره

۳۳۵۹ ۳۳۹۳ / ن ۸۵۱ / IIM

رده بندی دیویی

۳۰۳/۲۸۴۳

کتابشناسی ملی

۳۷۱۸۴۹۴



نشر فرهنگ روز

تهران، خ انقلاب، منیری جاوید(اردیبهشت)، بن بست توحید، پلاک ۴، نشر فرهنگ روز تلفن ۶۶۴۶۹۳۳۸

نام کتاب: هویت و امنیت سایبری

مؤلف : غلامرضا نخعی نیازی

ناشر: فرهنگ روز

شمارگان : ۱۰۰۰ نسخه

نوبت چاپ : اول - ۱۳۹۴

لیتوگرافی : جاووش

قیمت : ۱۵۰۰۰ تومان

شابک : ۶-۲۶-۶۳۳-۶۰۰-۹۷۸

حق چاپ محفوظ و مخصوص ناشر است.

مراکز پخش:

تهران، خ انقلاب، منیری جاوید(اردیبهشت)، بن بست توحید، پلاک ۴، نشر فرهنگ روز

تلفن ۶۶۴۸۲۸۰۴-۶۶۴۶۹۳۳۸

مقدمه مؤلف

امروزه بخش زیادی از کار و زندگی ما با الکترونیک، دیجیتال و فضای مجازی (سایبر) گره خورده است و روز به روز به انواع خدمات پولی یا رایگان این حوزه وابسته‌تر می‌شویم. هر یک از ما به حدی در فناوری سایبری غرق شده‌ایم که فراگیری حداقل نکات امنیتی لازم را از یاد برده‌ایم و تعداد کمی از ما برای مقابله با تهدیدات و آمادگی در شرایط خاص، تدبیر و برنامه مدون و موثری داریم. آیا تاکنون به درستی یا نادرستی رابطه زیر اندیشیده‌اید؟

وابستگی بیشتر به تجهیزات و ارتباطات سایبری = افزایش میزان آسیب پذیری

مثلاً در یک مقیاس کوچک، شما به موبایل خود خیلی وابسته هستید. اگر در آغاز یک روز کاری و پرمسئولیت، موبایل شما ویروسی، سرقت یا مفقود شود، چقدر به کار شما لطمه وارد می‌شود؟ چه آینده‌نگری می‌توانست در یک چنین شرایط خاصی، کمترین استرس و خسارت را به شما وارد کند؟

رابطه مستقیم این وابستگی و آسیب‌پذیری در مقیاس بزرگ‌تر، نگران‌کننده‌تر است. یعنی اگر زیرساخت‌ها و امکانات سخت‌افزاری کشور ما در حوزه ارتباطات و سایبر، پیش‌بینی‌های لازم را نداشته و خود را به شرایط خودکفایی و استقلال نزدیک نکرده باشد، شدت و وسعت آسیب‌پذیری در برابر تهدید مهاجمان و بحران‌های ساختگی، افزایش یافته و خسارات وارده، غیرقابل جبران خواهد بود. بنابراین لازم است تا متولیان فضای مجازی از یک سو و کاربران از سوی دیگر، دانش و فناوری بومی لازم را به‌منظور دفع، خنثی‌سازی و کاهش تأثیر انواع تهدیدات سایبری، داشته باشند.

هر آینده‌نگری و تلاش غیرمسلحانه من، شما و متولیان امر، که نوعی تدبیر و آمادگی برای مقابله با تهدیدات و بحران‌های احتمالی در فضای مجازی محسوب شود به نام **پدافند غیرعامل سایبری**^۱ می‌شناسیم. در این بین، وظیفه ملی هر یک از ما کاربران عادی، در نخستین گام، فراگیری حداقل دانش لازم است تا فرد دست و پا بسته و ناتوانی نباشیم.

افرادی که به دنبال فراگیری حداقل آموزش‌ها نبوده‌اند در برابر تهاجمات و تهدیدات سایبری به شکل ناخواسته و ندانسته، همان کاری را انجام می‌دهند که مهاجم یا مهاجمان قصد انجام آن را دارند. ایرانی بصیر، متعهد، متعصب و غیور، باید تلاش کند تا ناخواسته به خود و کشورش خسارتی وارد نکند. پیشاپیش از راهنمایی کارشناسان، اساتید، دانشجویان و علاقه‌مندان به موضوع امنیت سایبری، در رفع

نقایص این کتاب تشکر می‌کنم. www.icsbook.ir

مقدمه ناشر

تألیف و تحقیق، تنها بخش کوچکی از موضوع اطلاع‌رسانی و آموزش است. کلاس‌های آموزشی، برنامه‌های تلویزیونی، بسته‌های آموزشی و ضمیمه‌های فرهنگی و همایش‌ها و سمینارهای مختلف، از سوی متولیان امنیت و فضای سایبری، هریک به نوبه خود بخشی از بار آموزش، اطلاع‌رسانی و فرهنگ‌سازی را به دوش می‌کشند.

نکته قابل توجه در این میان، اهمیت آموزش به هنگام مخاطبان مبتدی در گروه‌های سنی مختلف است که هرروز به تعداد آن‌ها افزوده‌شده و فناوری جدیدتری در اختیار آن‌ها قرار می‌گیرد و در معرض تهاجمات سایبری بیشتری هستند و دلایلی مانند سن کم، عدم آشنایی با زبان انگلیسی و یا حتی مشغله زندگی و بی‌توجهی و بی‌حوصلگی این عزیزان، آموزش متمرکز و مؤثر آن‌ها را دشوار کرده است.

امروزه شاهدیم که، پیشرفت علوم رایانه‌ای، نرم‌افزارها و تجهیزات مرتبط با آن، به حدی سریع و برق‌آسا است که هر محتوای آموزشی با اهداف بهره‌وری یا پیشگیری، تاریخ‌مصرف محدودی داشته و حتی زمانی به دست مخاطبان می‌رسد که اصطلاحاً کار از کار گذشته و خسارت‌های زیادی به بار آمده است.

این کتاب نیز تلاش یک‌ساله‌ای است که جز با عنایت خداوند به ثمر نرسیده و بدون توجه و حمایت متولیان و مسئولان دلسوز کشورمان، هرگز در زمان مناسب به دست مخاطبان هدف نخواهد رسید.

انتشارات فرهنگ روز

فهرست

۵	فهرست
۱۴	انگیزه تألیف icsbook
۱۵	مخاطبان ics book
۱۶	گروه‌بندی سنی مخاطبان
۱۷	گروه بندی مهارتی کاربران
۱۸	فصل ۱ اصطلاحات سایبری
۱۹	هویت و امنیت سایبری یعنی چه؟
۲۰	واژه‌های ترکیبی از کلمه سایبر
۲۱	پدافند غیرعامل سایبری
۲۲	فضای سایبر به زبان ساده
۲۳	آزادی بدون مرز در فضای سایبر
۲۴	مفهوم آنالوگ و دیجیتال (رقمی)
۲۵	فناوری دیجیتال و فضای سایبر
۲۶	مثالی از یک فضای سایبر کوچک
۲۷	مثالی از فضای سایبر با شعاع بیشتر
۲۸	مثالی از یک فضای سایبر گسترده
۲۹	آیا فضای سایبر همان اینترنت است؟
۳۰	ارتباط اعداد با هویت کاربران
۳۱	تشخیص هویت در فضای سایبر
۳۲	لزوم افشای هویت
۳۳	انواع هویت در فضای مجازی
۳۴	هویت دیجیتال
۳۵	اثبات هویت در فضای سایبر
۳۶	سرقت هویت
۳۷	نمونه هایی از سرقت هویت دیجیتالی
۳۸	هویت مهاجمان سایبری
۳۹	امنیت سایبری
۴۰	تهدید سایبری
۴۱	پلیس سایبری

فصل ۲ اطلاعات مهم و حفاظت از آن‌ها..... ۴۲

- ۴۳.....چند توصیه مهم به مخاطبان خاص
- ۴۴.....حفاظت از اطلاعات چه ارتباطی با امنیت ما دارد؟
- ۴۵.....اطلاعات مهم یعنی کدام اطلاعات؟
- ۴۶.....انگیزه حفاظت از اطلاعات مهم.....
- ۴۷.....مفهوم طبقه‌بندی اطلاعات با ذکر مثال.....
- ۴۸.....مثال از حفظ اطلاعات شخصی و خصوصی.....
- ۴۹.....مثال از حفظ اطلاعات شغلی.....
- ۵۰.....مثال از حفظ اطلاعات ملی.....
- ۵۱.....فناوری ذخیره‌سازی دیجیتال اطلاعات.....
- ۵۲.....شما اطلاعات خود را کجا ذخیره می‌کنید؟
- ۵۳.....انواع ذخیره و نگهداری اطلاعات.....
- ۵۴.....سرقت نرم اطلاعات یا مهندسی اجتماعی.....
- ۵۵.....هوشیاری در فضای مجازی.....
- ۵۶.....حفاظت فیزیکی از اطلاعات یعنی چه؟
- ۵۷.....انواع خطرات فیزیکی.....
- ۵۸.....نکات حفاظت فیزیکی در محل کار.....
- ۵۹.....نکات حفاظت فیزیکی در اماکن عمومی.....
- ۶۰.....حفاظت فیزیکی از حافظه‌ها.....

فصل ۳ جرم سایبری و رایج‌ترین جرائم..... ۶۱

- ۶۲.....جرم سایبری یا رایانه‌ای.....
- ۶۳.....مصادیق جرائم سایبری.....
- ۶۴.....مهاجم کیست و به دنبال چیست؟
- ۶۵.....برداشت غیرمجاز و سرقت از حساب بانکی.....
- ۶۶.....هتک حیثیت.....
- ۶۷.....سرقت اطلاعات.....
- ۶۸.....تهدیدات.....
- ۶۹.....کلاهبرداری.....
- ۷۰.....سرقت رایانه‌ای.....
- ۷۱.....سرقت پول از طریق عابر بانک.....

۷۲.....	سرقت اطلاعات از طریق وای فای رایگان.....
۷۳.....	سرقت رمز عبور.....
۷۴.....	سرقت اینترنتی از حساب بانکی.....
۷۵.....	جمع‌آوری اطلاعات از طریق تلفن.....
۷۶.....	اغفال کاربران در فیس بوک (fb).....
۷۷.....	جعل هویت در فضای سایبر.....
۷۸.....	هک و نفوذ به رایانه و موبایل.....
۷۹.....	استفاده از سیمکارت دیگران.....
۸۰.....	پیامکهای فریب.....

فصل ۴ کلمات پرکاربرد به زبان ساده..... ۸۲

۸۳.....	data.....
۸۴.....	link.....
۸۵.....	Button.....
۸۶.....	Application.....
۸۷.....	hardware.....
۸۸.....	Software.....
۸۹.....	Operating System.....
۹۰.....	malware.....
۹۱.....	Computer.....
۹۲.....	Internet - intranet.....
۹۳.....	Connect to net.....
۹۴.....	Wireless - Wi MAX - Wi-Fi.....
۹۵.....	Network.....
۹۶.....	Access.....
۹۷.....	Share.....
۹۸.....	Home Network.....
۹۹.....	Bluetooth.....
۱۰۰.....	Bluetooth network.....
۱۰۱.....	U.R.L.....
۱۰۲.....	Domain.....

۱۰۳	vpn
۱۰۴	IP
۱۰۵	Download - Upload
۱۰۶	Hack - Hacker
۱۰۷	Web Browser
۱۰۸	pop-up
۱۰۹	Phishing
۱۱۰	Fake page
۱۱۱	Type
۱۱۲	exe
۱۱۳	User - User name
۱۱۴	USB
۱۱۵	Backup
۱۱۶	Update - upgrade
۱۱۷	firewall
۱۱۸	SSL

فصل ۵ امنیت در رایانه افلاین ۱۱۹

۱۲۰	امنیت ، یک فرایند است
۱۲۱	مهمترین و نخستین نرم افزار حیاتی.....
۱۲۲	استفاده درست از آنتی ویروس.....
۱۲۳	جلوگیری از اجرای خودکار ویندوز.....
۱۲۴	انتخاب نام مناسبی برای رایانه
۱۲۵	داشتن کلمه عبور
۱۲۶	ساختن رمز عبور مطمئن
۱۲۷	مراقبت در اتصال حافظه های جانبی
۱۲۸	قفل کردن اطلاعات مهم
۱۲۹	حفاظت از رایانه آماده به کار.....
۱۳۰	مدیریت امنیت رایانه مشترک
۱۳۱	آشنایی با مفاهیم حذف و ریکاوری.....
۱۳۲	لزوم آشنایی ویروس هیدن (Hidden).....

فصل ۶ امنیت تلفن همراه و تبلت ۱۳۳

- ۱۳۴ امنیت موبایل و تبلت را جدی بگیریم
- ۱۳۵ یک مثال از حفاظت فیزیکی
- ۱۳۶ رئوس نکات امنیتی لازم
- ۱۳۷ IMEI دستگاه ما چه عددی است؟
- ۱۳۸ پرهیز از بی‌نظمی در ذخیره اطلاعات
- ۱۳۹ تهیه نسخه پشتیبان از اطلاعات
- ۱۴۰ رمزنگاری اطلاعات حافظه موبایل
- ۱۴۱ رمزگذاری اطلاعات کارت‌های حافظه
- ۱۴۲ آینده نگری قبل و پس از سرقت
- ۱۴۳ در تحویل سیم کارت یا گوشی عجله نکنید
- ۱۴۴ هوشیاری در استفاده از بلوتوث
- ۱۴۵ برده داری سایبری با موبایل

فصل ۷ بانکداری مجازی ۱۴۷

- ۱۴۸ یک حساب بانکی چند شماره مرتبط دارد؟
- ۱۴۹ رمزهای چهاررقمی متفاوت
- ۱۵۰ رمزهای پنج رقمی متفاوت
- ۱۵۱ چگونه رمزهای متفرقه بسازیم
- ۱۵۲ شماره‌های مهم خود را نامرئی کنیم
- ۱۵۳ در استفاده از رمز باید هوشیار بود
- ۱۵۴ اینترنت بانک
- ۱۵۵ صفحات جعلی اینترنت بانک
- ۱۵۶ چگونه نشانی اصلی بانک را بشناسیم؟
- ۱۵۷ عابر بانک
- ۱۵۸ آموزش افراد مبتدی خانواده
- ۱۵۹ آشنایی با محدودیت عملیات خودپردازها
- ۱۶۰ توجه به علائم مشکوک در خودپردازها
- ۱۶۰ نکات مهم تا رسیدن به خودپرداز
- ۱۶۲ مهم‌ترین نکات دریافت یا انتقال پول
- ۱۶۳ راه‌های مسدود کردن کارت بانکی

۱۶۴	 پایانه فروش
۱۶۵	 جانمایی و استفاده صحیح از کارت خوان
۱۶۶	 اهمیت رسید جایی در تراکنش ها
۱۶۷	 بروز مشکلات فنی و ظاهری در پایانه ها
۱۶۸	 از شگردهای سرقت توسط POS
۱۶۹	 همراه بانک
۱۷۰	 نکات امنیتی استفاده از همراه بانک
۱۷۱	 همبانک
۱۷۲	 امنیت استفاده از همبانک
۱۷۳	 تلفن بانک
۱۷۴	 امنیت استفاده از تلفن بانک
۱۷۵	 خرید اینترنتی
۱۷۶	 نگرانی های یک خرید اینترنتی
۱۷۷	 نشانه های فروشگاه اینترنتی معتبر
۱۷۸	 نماد اعتماد الکترونیکی یا اینماد
۱۷۹	 بهترین روش پرداخت در خریدهای آنلاین
۱۸۰	 شناخت درگاه جعلی پرداخت بانک
۱۸۱	 حواله بانکی روشی غلط در خرید اینترنتی
۱۸۲	 مهم ترین نکات قبل از خرید اینترنتی

فصل ۸ امنیت در وبگردی ۱۸۳

۱۸۴	 مشخصات مستعار در وبگردی
۱۸۵	 مدیریت عضویت در وبسایت ها
۱۸۶	 وبگردی با استفاده از رایانه دیگر
۱۸۷	 خطرات و خدمات کافی نت
۱۸۸	 ردپای ما در کافی نت
۱۸۹	 یک مرورگر امن انتخاب کنیم
۱۹۰	 تنظیمات امنیتی مرورگر
۱۹۱	 مدیریت پلاگین های مرورگر
۱۹۲	 به روزرسانی مرورگر الزامی است
۱۹۳	 مدیریت و پایش مستمر ترافیک

۱۹۴	 استفاده مستمر از کوکی‌ها اشتباه است
۱۹۵	 مدیریت رمزهای عبور
۱۹۶	 نادیده گرفتن پیام‌ها و پنجره‌های <i>Popup</i>
۱۹۷	 خطر دکمه‌های پنجره پاپ آپ
۱۹۸	 کلیک دزدی از کاربران
۱۹۹	 دامی در قالب تصاویر زیبای فلش
۲۰۰	 پسوند آگزه (.exe) خطرناک‌ترین فایل
۲۰۱	 حفظ سلامت رایانه بدون هزینه ؟
۲۰۲	 مدیریت یا بستن وب کم
۲۰۳	 یکی از راه‌های کنترل از راه دور رایانه
۲۰۴	فصل ۹ ایمیل و رایانش ابری
۲۰۵	 مالکیت و امنیت ایمیل
۲۰۶	 حتماً برای خود ایمیل داشته باشیم
۲۰۷	 انتخاب یک سرویس دهنده امن
۲۰۸	 ایمیل را خودمان ثبت کنیم
۲۰۹	 عبور از فرم‌های کنجکاو عضویت
۲۱۰	 محافظت از ایمیل اصلی
۲۱۱	 ایمیل عضویت چیست ؟
۲۱۲	 حقه‌ای به نام لینک تأیید
۲۱۳	 محافظت از رمز عبور ایمیل
۲۱۴	 محافظت از ایمیل در کافی‌نت‌ها
۲۱۵	 فایل‌های پیوست مخرب در ایمیل
۲۱۶	 ایمیل‌های پوشه اسپم (<i>Spam</i>)
۲۱۷	 از روش‌های متداول سرقت پسورد
۲۱۸	 نشانه‌های ورود مهاجم به ایمیل ما
۲۱۹	 نجات سریع حساب‌های کاربری
۲۲۰	 سایر نکات امنیتی کار با ایمیل
۲۲۱	 رایانش ابری
۲۲۲	 مثال‌هایی از رایانش ابری
۲۲۳	 امنیت در رایانش و مکاتبات ابری

فصل ۱۰ شبکه‌های اجتماعی ۲۲۴

- ۲۲۵ مفهوم شبکه اجتماعی
- ۲۲۶ شما چند شبکه اجتماعی می‌شناسید؟
- ۲۲۷ شبکه‌های اجتماعی ، بد یا خوب؟
- ۲۲۸ شبکه‌های اجتماعی ، دوست یا جاسوس؟
- ۲۲۹ شبکه‌های اجتماعی در ایران
- ۲۳۰ بزرگ‌ترین خدمت به شبکه‌های اجتماعی

- ۲۳۱ الف (نکات امنیتی مشترک
- ۲۳۲ کاربر هوشیاری باشیم
- ۲۳۳ در اینترنت به روز باشید
- ۲۳۴ (App) اپلیکیشن های رایگان و خیر خواه ؟
- ۲۳۵ رمز عبور مطمئن برای حساب کاربری
- ۲۳۶ راه‌های سرقت رمز حساب کاربری
- ۲۳۷ سرقت رمز عبور در فرایند ثبت نام
- ۲۳۸ دام‌های فیشینگ
- ۲۳۹ لینک ها ، عکس ها و پیوست های آلوده
- ۲۴۰ شناخت اهداف گروه های خاص
- ۲۴۱ اطمینان از هویت سایر اعضا
- ۲۴۲ عدم اعتماد به دوستان مجازی
- ۲۴۳ محافظت از اطلاعات محرمانه
- ۲۴۴ راست و دروغ اخبار منتشره
- ۲۴۵ تحقیق بیشتر در مورد محتوای مشکوک
- ۲۴۶ چیزی برای گفتن باقی مانده ؟
- ۲۴۷ اهمیت توجه والدین به نسل جدید

۲۴۸.....	ب) نکات اخلاقی مشترک
۲۴۹.....	تعیین مرزهای اخلاقی
۲۵۰.....	مثالی از تعیین مرزهای اخلاقی
۲۵۱.....	تعیین مرزهای اخلاقی در اینترنت
۲۵۲.....	اندوخته‌های ما و تعیین مرزهای امروز
۲۵۳.....	مرزی به نام حریم خصوصی
۲۵۴.....	اینترنت همه زندگی من!
۲۵۵.....	زندگی انفرادی من
۲۵۶.....	شخصیت مجازی من
۲۵۷.....	مدیریت زندگی مجازی
۲۵۸.....	دوست‌یابی در شبکه‌های اجتماعی
۲۵۹.....	انتخاب همسر در شبکه‌های اجتماعی
۲۶۰.....	پرهیز از قرار حضوری با دوستان مجازی
۲۶۱.....	خودداری از انتشار شایعات
۲۶۲.....	عامل ایجاد فیلترینگ کیست؟
۲۶۳.....	شناخت اهداف و علاقه‌مندی‌های دیگران
۲۶۴.....	حفظ حرمت ادیان و مذاهب مختلف
۲۶۵.....	خودداری از توهین به خود و هم‌وطنان
۲۶۶.....	تأسف از دست دادن هویت
۲۶۷.....	تغییر تفکر و سطح توقع کاربران
۲۶۸.....	انتقاد، توأم با ظرفیت انتقادپذیری
۲۶۹.....	حفظ ارزش‌های خانواده
۲۷۰.....	پرهیز از محتوای غیراخلاقی
۲۷۱.....	پیوست ۱: سیاست‌های کلی نظام در امور (آفتا)